PURPOSE

To protect Michigan Department of Health and Human Services (MDHHS) information systems and assets through controlling physical access and implementing controls to protect the environment in which agency information systems and assets are located.

REVISION HISTORY

Issued: 1/01/2020.
Next Review: 1/01/2021.

DEFINITIONS

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an Agency or the SOM. Confidential data may include personally identifying information (PII) or confidential non-public information that relates to an Agency’s business.

Criminal Justice Information (CJI)

Federal Bureau of Investigation (FBI) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Electronic Protected Health Information (ePHI)

Protected Health Information transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the Internal Revenue Service (IRS).

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

Protected Health Information (PHI)

Individually identifiable health related information that is collected by a HIPAA covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

SSA-Provided Information

Confidential information provided by the Social Security Administration (SSA).

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

MDHHS must apply and manage physical security safeguards to prevent unauthorized communication or transmission access, maintain access records, minimize the compromise of sensitive output information, and protect SOM equipment, facilities and environments.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the physical and environmental protection [PE] family of NIST controls, managed by MDHHS in accordance with DTMB 1340.00.120.01, Physical and Environmental Protection Standard. MDHHS must review this policy annually.

Where applicable, this policy requires compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities
- Social Security Administration (SSA) Technical System Security Requirements (TSSR)
- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C

Physical Access Authorizations [PE-2]*

MDHHS must:

- Issue authorization credentials for facility access.
- Maintain lists of individuals with authorized access and review at least once every 180 days.
- Timely remove individuals from the facility access list when access is no longer required.

Access by Position/Role [PE-2(1)]

MDHHS must ensure that facility access authorization does not exceed the level required for a workforce member’s position, role and/or job responsibilities.

Physical Access Control [PE-3]*

MDHHS must:

- Restrict access to areas within facilities as follows:
    - For areas officially designated as publicly accessible, through the use of barriers, cameras, monitoring by

guards, and isolation of selected information systems and/or system components in secured areas.

  - For areas where PII and/or servers are maintained, through multiple barriers, including but not limited to secured/locked perimeter, security room, and/or locked/security container.

- Enforce physical access authorizations at entry/exit points to the facility where the information system resides by:

  - Verifying individual access authorizations before granting access to the facility.

  - Controlling ingress/egress to the facility using physical access control systems/devices and guards.

- Maintain physical access audit logs for defined entry/exit points.

- Escort visitors and monitors visitor activity in all circumstances within restricted access area where the information system resides.

- Secure keys, combinations, and other physical access devices.

- Inventory physical access devices, including but not limited to keys, locks, combinations, and card readers. at least annually.

- Change combinations and keys at least annually and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

- Utilize and periodically update physical access control systems to comply with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.

Access Control for Output Devices [PE-5]

MDHHS must control physical access to information system output devices, including, but not limited to, monitors, printers, copiers, scanners, facsimile machines, projectors, and audio devices, to prevent unauthorized individuals from obtaining the output.

Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel.

Monitoring Physical Access [PE-6]

MDHHS must review safeguards and supporting procedures to:

- Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.

- Review physical access logs at least monthly and upon occurrence of suspicious activity or persons.

- Coordinate results of reviews and investigations with the SOM incident response capability.

Visitor Access Records [PE-8]*

MDHHS must maintain visitor access records for each facility for at least a year and be reviewed on at least a monthly basis.

Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited.

Visitor access records are not required for publicly accessible areas.

Alternate Work Site [PE-17]

With local (non-DTMB-managed) facilities, MDHHS must:

- Deploy appropriate security controls, including those supporting contingency planning activities, at alternate work sites, including, but not limited to, government facilities or private residences of employees.

- Assess, as feasible, the effectiveness of security controls at alternate work sites.

- Communicate with information security personnel in case of security incidents or problems.

ROLES AND RESPONSIBILITIES

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for:

- Keeping all external doors closed at all times.
- Locking internal doors to secured areas when unattended.
- Escorting visitors obtaining access to controlled access areas.
- Reading, understanding and complying with the requirements detailed in this and other Information Security Program policies.
- Following procedures to address general operation of facilities.
- Reporting violations of this policy.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

Federal Standards/Regulations

NIST 800-53 rev.4:

PE-1 Physical and Environmental Protection Policy and Procedures

PE-2 Physical Access Authorizations*
PE-3 Physical Access Control*
PE-5 Access Control for Output
PE-8 Visitor Access Records*
PE-17 Alternate Work Site

* Applicable to MDHHS-operated hospitals, centers, and facilities

45 CFR §164.310

164.310(a)(1) Facility Access Controls (R)
164.310(a)(2)(ii) Facility Security Plan (A)
164.310(a)(2)(iii) Access Control & Validation (A)
164.310(b) Workstation Use (R)
164.310(c) Workstation Security (R)
164.310(a)(2)(i) Contingency Operations (A)

State Standards/Regulations

DTMB Administrative Guide

DTMB/Work Resources/Policies, Standards and Procedures/IT Technical Policies, Standards and Procedures

210 Facilities Administration
400.05 Facility Security-ID/Access Card

1340.00.120.01 Physical and Environmental Protection Standard

CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.